UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/599,230	09/22/2006	Karl Asperger	78857.105107	6068

86528 7590 12/15/2011

King & Spalding LLP
401 Congress Avenue
Suite 3200
Austin, TX 78701

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
12/15/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

AustinUSPTO@kslaw.com
AustinIP@kslaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/599,230	ASPERGER ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/18/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/10/2010 has been entered.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 6/18/2010 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Response to Arguments

3. Claims 1 and 20 have been amended. No claim has been cancelled. No new claim has been added. Therefore, claims 1-20 are now pending.

4. Applicant's amendments are sufficient to overcome the claim rejections of claims 1 and 20, for USC 112 first paragraph rejections set forth in the previous office action. Applicant amended the independent claims 1 and 20 to remove the phrase of "a breach of the protective layer" for the limitation. Thus, the claim rejections of claims 1 and 20 for USC 112 first paragraph is withdrawn.

5. Applicant's arguments files on April 14, 2010 with respect to independent claims 1 and 20 (see Remark page 6-10) have been considered but are moot in view of the new

ground(s) of rejection. For example, Applicant amended the independent claim 1 and 20 to recite "including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security sensor system operable to monitor the state of the protective layer on the integrated circuit such that when a breaking of the electrical line is detected" which were not presented in any previous listing of the claim. Therefore, the scope of the claims has changed. Accordingly, new ground of rejection is being used to address the newly added limitation. Therefore, Applicant's arguments are rendered moot.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 13 is rejected under 35 U.S. C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites "wherein an active protective layer which consists of at least one elongated electrical line which extends along the surface of **the die**, particularly in mutually parallel tracks section by section, is applied directly to **the die** of the semiconductor chip." There is insufficient antecedent basis for the claim limitation.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-4, 6, 8-19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore (US 5,861,662) hereinafter Candelore, in view of Yamauchi et al (US 2002/0040420 A1), hereinafter Yamauchi.

As for claim 1:

Candelore discloses **an integrated circuit** (See Candelore Fig 1 element 100) **comprising function modules, wherein the function modules comprise a central processing unit designed to process data and to execute programs, and a cache memory, wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules** (See Candelore column 6 lines 12-18 "FIG. 3 is a top view illustrating, in simplified form, a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306.") **comprise a security sensor system including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security' sensor system operable to monitor the state of the protective layer on the integrated circuit such that when a breaking of the electrical line is detected, data is automatically deleted from at least one memory of the integrated circuit.** (See Candelore column 5 lines 12-30 "A shield 230 is a metal layer that

provides current to various components within the IC 200, such as the components 150-156 of FIG. 1. If power to the shield is interrupted, then a secure processing component may self-destruct such that cryptographic data which is stored in the secure processor is erased. Additionally, the shield 230 serves to prevent a pirate from using a scanning electron microscope to detect changes (e.g., voltage changes) in portions of the secure processor, such as a random access memory (RAM), and blurs the distinction between parts which are coated by the shield. The shield may be located within the encapsulating layer, which includes one or more protective layers which are disposed above the chip in the substrate 250. A passivation layer 240 is a protective surface coat comprising, for example, silicon dioxide which is deposited over the surface of the die during various diffusion steps. The substrate 250 is the physical material upon which the IC is fabricated or assembled. " and column 6 lines 31-40 "In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324. The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150.")

Candelore discloses an anti-tamper shield for an integrated circuit (IC) includes a bond wire which passes through a protective layer such as an epoxy encapsulating layer of the IC. The bond wire is carried within and/or proximate to the encapsulating layer such that a decapsulation of the IC will cause a rupture of the electrically conductive member,

thereby rendering the processor non-functional. A metallic shield layer may be located between the active component and a top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey the active component region. (See Candelore [abstract]) However, Candelore does not explicitly disclose "**a cache memory, wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules; "** as claimed. Yamauchi discloses as claimed (see Yamauchi [0296] "The microcomputer 90 includes: a CPU core 94; a cache memory 96; a memory controller 98; and an external bus interface circuit 100, wherein the constituents are connected to each other by an internal bus 102." And [0033]Fig 10 a fundamental unit for DES encryption used as a secrete key cryptosystem; [0083 Fig 60 a block diagram representing an example of a circuit configuration for performing encryption or decryption in the CBC mode**)** Therefore, it would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Candelore to include the cache memory of encryption unit for data encryption as taught by Yamauchi because they are analogous in the secure integrated circuit and one of ordinary skill in the art would have been motivated to incorporate the teaching and therefore achieve efficiency and fragility with existing silicon technology. (see Yamauchi [0146])

As for claim 2:

The combination of Candelore and Yamauchi teaches **the integrated circuit according to claim 1, wherein the function modules comprise a random-number generator.** (see Yamauchi [0599]" A secrete key cryptosystem which can be used is

notified and a random number and a current time point is sent to the host side. [0600] 6) The host side determines a secret key cryptosystem and notifies the client side of which secrete key cryptosystem is adopted and obtains the random number and the current time point . [0601] The client generates random numbers serving as a base of a secret key. [0602] The random numbers generated are enciphered with the public key of the server and thereafter sent to the server.)

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 3:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1, wherein function modules comprise a first memory in which cryptological keys are stored.** (see Yamauchi [0470] and FIG 54 " At Y addresses #10 to #13, stored is a first key of 64 bits in length, and at Y address #14 to #17, stored is a second key of 64 bits in length.")

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 4:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 3, wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator.** (see Yamauchi [0598]-[0602])

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 6:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1, wherein operating parameters to be monitored additionally is the clock frequency of the real-time clock and/or an operating temperature at a point in the integrated circuit and/or an operating voltage of the integrated circuit.** (see Candelore column 6 lines 31-40 "In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324. The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150.")

As for claim 8:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1, wherein it is arranged in a package and has terminal contacts brought out of the package.** (see Yamauchi [0131] "Terminals of a chip 1 are the same as terminals used in a general purpose DRAM. Hence, the same package as in which a general purpose DRAM chip is housed can be employed. For example, a package in which the semiconductor integrated circuit device 1 is housed is one having a pin configuration as shown in FIG. 101.")

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 9:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1, none of them discloses wherein individual function modules have an essentially planar extent and are arranged adjacently to one another in the area of the normal to the surface.** (see Candelore column 4 lines 56-60 "a grid configuration may be used even when the wire does not carry an electrical signal which the processor requires to function.")

As for claim 10:

The combination of Candelore and Yamauchi discloses **the integrated circuit as according to claim 1, wherein the function modules comprise an integrated voltage regulator which regulates an operating voltage.** (see Candelore column 6 lines 31-40 "In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324.")

As for claim 11:

The combination of Candelore and Yamauchi discloses **the integrated circuit as according to claim 1, wherein it is constructed as semiconductor chip.** (see Candelore column 1 lines 35-43 "A secure processor includes an integrated circuit (IC) which is fabricated as a monolithic device with an ensemble of active and passive

components, including transistors, resistors, capacitors, and diodes which are interconnected within a monolithic block of semiconductor material. During probing, ICs such as very large scale integrated (VLSI) circuits are subject to an invasive attack wherein the die (e.g., IC or "chip") is exposed by decapsulation.")

As for claim 12:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 11, none of them discloses wherein semiconductor structures of the individual function modules are intermeshed in the manner of a puzzle in order to avoid individual function modules from being recognizable.** (see Candelore column 4 lines 50-60 "a mesh configuration, a configuration wherein a single wire is coupled to more than two terminals, or virtually any electrically conductive member. In particular, the wires may be provided in a grid pattern with a spacing which is small enough to prevent a probe from passing through the mesh or moving easily within the mesh, as discussed below in conjunction with FIG. 4. In fact, a grid configuration may be used even when the wire does not carry an electrical signal which the processor requires to function. The mere presence of the grid serves as a deterrent to probing. ") Candelore discloses the mesh configuration with the grid serves the deterrent to probing which teaches the manner of a puzzle in order to avoid individual function from being recognizable.

As for claim 13:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 11, none of them discloses wherein an active protective layer**

which consists of at least one elongated electrical line which extends along the surface of the die, particularly in mutually parallel tracks section by section, is applied directly to the die of the semiconductor chip. (see Candelore Fig 1 of the chip 100 and FIG4 and column 8 lines 1-11. In FIG 1 element 130 is the die and element 150 is the secure processor including the cryptographic information. In FIG 4, element 450 is the processor with the protect layer with the FIG 4 of a meshed grid with the parallel wire bond (element 421,423 and 425) which is elongated electrical line which extends along the surface of the die.)

As for claim 14:

The combination of Candelore and Yamauchi discloses **an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the integrated circuit is connected by means of a data bus to a second memory in which data are stored encrypted, wherein the second memory has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner.** (see Candelore column 6 lines 12-25 “a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306.”)

As for claim 15:

The combination of Candelore and Yamauchi discloses **the arrangement comprising an integrated circuit as claimed claim 14, but does not wherein the second memory is volatile and is connected to a battery so that the voltage supply is maintained when another power supply is lacking.** (see Candelore column 5 lines 49-55 "If a electrically conductive member is used in a component which did not have a battery powered erasure feature, then the electrically conductive member may instead carry various control signals.")

As for claim 16:

The combination of Candelore and Yamauchi discloses **an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the integrated circuit is connected by means of a data bus to a non-volatile third memory in which data or program code are stored encrypted.** (see Candelore column 6 lines 12-25 "a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306.")

As for claim 17:

The combination of Candelore and Yamauchi discloses **the arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the security sensor system is connected to a battery so that the voltage supply is maintained if another power supply is lacking.** (see Candelore column 2 lines 59-61"

This signal may include a steady state electrical current which is supplied by a battery via positive and negative terminals. The wire may be carried, at least in part, in a protective layer of the IC such that removal of the protective layer will rupture the wire, thereby causing an open circuit. “)

As for claim 18:

The combination of Candelore and Yamauchi discloses **the arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the security sensor system is connected to an auxiliary power source, integrated in the package, which provides the power for deleting the first memory.** (see Candelore column 1 lines 50-60 “If the chip requires a direct current from a battery or the like to circumvent a self-destruct feature, then battery wires are soldered to a positive voltage pin (e.g., V_{batt}) pin and to a negative voltage pin (e.g., V_{ss}) on the outside of the chip prior to removal from the board.”)

As for claim 19:

The combination of Candelore and Yamauchi discloses **an arrangement comprising an integrated circuit as claimed claim 16, wherein the third memory is a Flash memory or ROM.** (see Candelore column 8 lines 60-63 “the invention is not limited to use with chips which have an epoxy encapsulating layer, but may be adapted for use with a chip which has virtually any type of protective layer, or even no protective layer. For instance, the invention may be used with a device such as an electrically programmable read-only memory (EPROM), which can be erased when exposed to ultraviolet light.”)

As for claim 20:

Candelore discloses **an integrated circuit** (See Candelore Fig 1 element 100) **comprising function modules, wherein the function modules comprise a central processing unit designed to process data and to execute programs, and a cache memory, wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules** (See Candelore column 6 lines 12-18 "FIG. 3 is a top view illustrating, in simplified form, a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306.") **comprise a security sensor system including a protective layer on the integrated circuit including at least one elongated electrical line extending along the surface of the integrated circuit, the security sensor system operable to monitor the state of the protective layer on the integrated circuit such that when a breaking of the electrical line is detected, data is automatically deleted from at least one memory of the integrated circuit,** (See Candelore column 5 lines 12-30 "A shield 230 is a metal layer that provides current to various components within the IC 200, such as the components 150-156 of FIG. 1. If power to the shield is interrupted, then a secure processing component may self-destruct such that cryptographic data which is stored in the secure processor is erased. Additionally, the shield 230 serves to prevent a pirate from using a scanning

electron microscope to detect changes (e.g., voltage changes) in portions of the secure processor, such as a random access memory (RAM), and blurs the distinction between parts which are coated by the shield. The shield may be located within the encapsulating layer, which includes one or more protective layers which are disposed above the chip in the substrate 250. A passivation layer 240 is a protective surface coat comprising, for example, silicon dioxide which is deposited over the surface of the die during various diffusion steps. The substrate 250 is the physical material upon which the IC is fabricated or assembled. " and column 6 lines 31-40 "In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324. The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150.") **wherein the function modules comprise a random-number generator and a first memory in which cryptological keys are stored, and wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator.**

Candelore discloses an anti-tamper shield for an integrated circuit (IC) includes a bond wire which passes through a protective layer such as an epoxy encapsulating layer of the IC. The bond wire is carried within and/or proximate to the encapsulating layer such that a decapsulation of the IC will cause a rupture of the electrically conductive member, thereby rendering the processor non-functional. A metallic shield layer may be located

between the active component and a top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey the active component region. (See Candelore [abstract]) However, Candelore does not explicitly disclose "**a cache memory, wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules; "** and **"the function modules comprise a random-number generator and a first memory in which cryptological keys are stored, and wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator"** as claimed.

Yamauchi discloses as claimed (see Yamauchi [0296] "The microcomputer 90 includes: a CPU core 94; a cache memory 96; a memory controller 98; and an external bus interface circuit 100, wherein the constituents are connected to each other by an internal bus 102." And [0033]Fig 10 a fundamental unit for DES encryption used as a secrete key cryptosystem; [0083 Fig 60 a block diagram representing an example of a circuit configuration for performing encryption or decryption in the CBC mode and Yamauchi [0599]" A secrete key cryptosystem which can be used is notified and a random number and a current time point is sent to the host side. [0600] 6) The host side determines a secret key cryptosystem and notifies the client side of which secrete key cryptosystem is adopted and obtains the random number and the current time point . [0601] The client generates random numbers serving as a base of a secret key. [0602] The random numbers generated are enciphered with the public key of the server and thereafter sent to the server. and further in [0470] and FIG 54 " At Y addresses #10 to

#13, stored is a first key of 64 bits in length, and at Y address #14 to #17, stored is a second key of 64 bits in length.")

Therefore, it would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Candelore to include the cache memory of encryption unit for data encryption as taught by Yamauchi because they are analogous in the secure integrated circuit and one of ordinary skill in the art would have been motivated to incorporate the teaching and therefore achieve efficiency and fragility with existing silicon technology. (see Yamauchi [0146])

10. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore and Yamauchi as applied to claims 1 above, further in view of Nakajima et al (US 2004/0106239 A1), hereinafter Nakajima.

As for claim 5:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1**, neither Candelore nor Yamauchi discloses **wherein function modules comprise a real-time clock.**

However, Nakajima discloses wherein function modules comprise a real-time clock. **(see Nakajima [0098] "circuitry 510 including a real-time clock, a serial interface, and a timer, a clock control circuit 511, a cache controller 512, and a bus controller 513 are formed on the dielectric film.")**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to include the teaching of Nakajima within the integrated circuit using real-time clock to the modified-invention of Candelore because they are

analogous in the secure microprocessor. One of the ordinary skill in the art would have been motivated to incorporate the teaching of real-time clock to provide benefit for real-time information for the security sensor in the event of an attack being detected and therefore achieve efficiency and fragility with existing silicon technology.

11. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore and Yamauchi as applied to claims 1 above, further in view of Anderson et al (US 2003/0084336 A1) hereinafter Anderson.

As for claim 7:

The combination of Candelore and Yamauchi discloses **the integrated circuit according to claim 1**, neither Candelore nor Yamauchi discloses **wherein at least one limit value is predetermined for the operating parameter to be monitored, the operating parameter is measured and compared with the limit value and when the result exceeds or drops below the limit value, the content of the first memory is deleted.** However, Anderson discloses as claimed. (see Anderson [0014]" One sensor in our invention is based on an instruction counter; the processor software can check that the expected number of instructions have been executed and alarm if this is riot the case (as might happen, for example, under destructive probing attack). Other sensors are outside the scope of this patent but may typically be designed to detect out-of-bounds environmental parameters such as over- and under-voltage and low temperature." and [0015]" Once an alarm signal has been injected into the data-path it obliterates the data in the pipeline since any dyadic function of a valid logic level with an alarm signal will result in an alarm signal.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the modified-invention of Candelore to include operating parameter measure as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in the modified-invention of Candelore of using operating measure for sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve efficiency and fragility with existing silicon technology.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kömmerling et al (US 2001/0033012 A1)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. L./
Examiner, Art Unit 2438
/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438